Featured news

US charges Sandworm hackers who mounted NotPetya, other high-profile attacks

Can we trust passwordless authentication?

What is confidential computing? How can you use it?

SecOps teams turn to next-gen automation tools to address security gaps

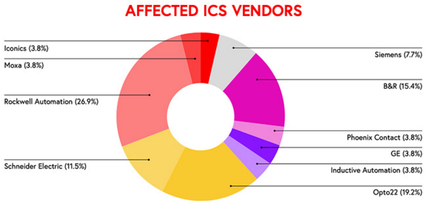
Is poor cyber hygiene crippling your security program?

Industry News
August 20, 2020

Share

Most ICS vulnerabilities disclosed this year can be exploited remotely

More than 70% of ICS vulnerabilities disclosed in the first half of 2020 can be exploited remotely, highlighting the importance of protecting internet-facing ICS devices and remote access connections, according to Claroty.



The report comprises The Claroty Research Team's assessment of 365 ICS vulnerabilities published by the National Vulnerability Database (NVD) and 139 ICS advisories issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) during 1H 2020, affecting 53 vendors. The research team discovered 26 of the vulnerabilities included in this data set.

Compared to 1H 2019, ICS vulnerabilities published by the NVD increased by 10.3% from 331, while ICS-CERT advisories increased by 32.4% from 105. More than 75% of vulnerabilities were assigned high or critical Common Vulnerability Scoring System (CVSS) scores.

"There is a heightened awareness of the risks posed by ICS vulnerabilities and a sharpened focus among researchers and vendors to identify and remediate these vulnerabilities as effectively and efficiently as possible," said Amir Preminger, VP of Research at Claroty.

"We recognized the critical need to understand, evaluate, and report on the comprehensive ICS risk and vulnerability landscape to benefit the entire OT security community.

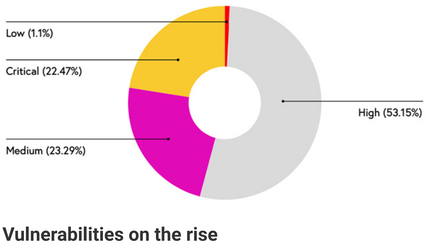
"Our findings show how important it is for organizations to protect remote access connections and internet-facing ICS devices, and to protect against phishing, spam, and ransomware, in order to minimize and mitigate the potential impacts of these threats."

Prominence of RCE vulns highlights need to protect internet-facing ICS devices

According to the report, more than 70% of the vulnerabilities published by the NVD can be exploited remotely, reinforcing the fact that fully air-gapped ICS networks that are isolated from cyber threats have become vastly uncommon.

Additionally, the most common potential impact was remote code execution (RCE), possible with 49% of vulnerabilities – reflecting its prominence as the leading area of focus within the OT security research community – followed by the ability to read application data (41%), cause denial of service (DoS) (39%), and bypass protection mechanisms (37%).

The prominence of remote exploitation has been exacerbated by the rapid global shift to a remote workforce and the increased reliance on remote access to ICS networks in response to the COVID-19 pandemic.



Vulnerabilities on the rise

The energy, critical manufacturing, and water & wastewater infrastructure sectors were by far the most impacted by vulnerabilities published in ICS-CERT advisories during 1H 2020.

Of the 385 unique Common Vulnerabilities and Exposures (CVEs) included in the advisories, energy had 236, critical manufacturing had 197, and water & wastewater had 171. Compared to 1H 2019, water & wastewater experienced the largest increase of CVEs (122.1%), while critical manufacturing increased by 87.3% and energy by 58.9%.

Assessment of ICS vulnerabilities discovered

The research team discovered 26 ICS vulnerabilities disclosed during 1H 2020, prioritizing critical or high-risk vulnerabilities that could affect the availability, reliability, and safety of industrial operations.

The team focused on ICS vendors and products with vast install bases, integral roles in industrial operations, and those that utilize protocols in which researchers have considerable expertise. These 26 vulnerabilities could have serious impacts on affected OT networks, because more than 60% enable some form of RCE.

More about

Claroty | CVE | CVSS | cybersecurity | ICS/SCADA | remote access | vulnerability | vulnerability disclosure

Share this

Can we trust passwordless authentication?

Review: Netsparker Enterprise web application scanner

New research shows risk in healthcare supply chain

What is confidential computing? How can you use it?

What's new

Is poor cyber hygiene crippling your security program?

US charges Sandworm hackers who mounted NotPetya, other high-profile attacks

SecOps teams turn to next-gen automation tools to address security gaps

Can we trust passwordless authentication?

Don't miss

US charges Sandworm hackers who mounted NotPetya, other high-profile attacks

Can we trust passwordless authentication?

What is confidential computing? How can you use it?

SecOps teams turn to next-gen automation tools to address security gaps

Magento, Visual Studio Code users: You need to patch!

© Copyright 1998-2020 by Help Net Security